

## Task 1

Nmap Analysis for IP address 162.241.219.170 elixir.com.sg

Open ports:

993/tcp

2222/tcp

3306/tcp

5432/tcp

Operating system used:

Dell DR4100 backup appliance (89%),

FreeBSD 6.2-RELEASE (89%),

Android TV OS 11 (Linux 4.19) (89%),

Android 7.1.2 (Linux 3.10) (89%)

## Task 2

Locate vulnerabilities found:

No vulnerabilities found

## Task 3

List the Open ports, service version and vulnerabilities that could occur in each port?

993/tcp, Service Version: Dovecot imapd; Vulnerabilities could include: Possible remote code execution or information disclosure due to improper handling of SSL/TLS connections.

2222/tcp, Service Version: OpenSSH 7.4 (protocol 2.0); Vulnerabilities could include: Information leak in roaming features(client side)

3306/tcp, Service Version: MySQL 5.7.23-23; Vulnerabilities could include: Remote attackers can perform arbitrary code execution via a certain MySQL component

5432/tcp, Service Version: PostgreSQL DB; Vulnerabilities could include: PostgreSQL mishandles large tables, which could lead to unauthorized access to stored data

